

SEAMEO INNOTECH DATA PRIVACY POLICY

General

SEAMEO INNOTECH adopted this Privacy Policy to stress the Center's commitment to protect data and personal information that are given by staff, partners, participants, clients and other interested parties. The Center ensures that all collected personal data are processed in adherence to the general principles of transparency, legitimate purpose and proportionality.

This policy is intended to guide the Center's staff and partners in ensuring that sensitive personal information, as well as photo, video and audio documentation during Center activities gathered are treated with utmost care and sensitivity.

Collection of Data

The Center collects, acquires, generates and manages personal data in many forms from staff, partners, participants, consultants, stakeholders and other interested parties for various organizational purposes. They may consist of written records, photographic images, video footages or digital materials. In the course of Center operations, certain information may be collected such as, but not limited to – name, present address, birthday, contact information, educational background, work details, related work experience, etc. In addition, the Center may also collect or generate additional information after registration and during actual activities. There may also be circumstances when the Center will collect other forms of data like digital photos and videos of activities as part of the Center's documentation requirements, or through recordings from closed-circuit television cameras installed within the Center premises for safety and security purposes.

Use of Personal Information

Unless otherwise stated, personal information gathered is accessed, used and processed by the Center and authorized personnel who have legitimate interests in it for the intention of carrying out their duties and responsibilities. The personal data contained in information/ registration forms and on any supplementary documents may be used for a variety of academic, administrative, historical and statistical purposes, including the following:

- for profiling related to needs analysis activities;
- for use in Center-generated reports, documents, publications and audio-video productions/presentations;
- for inclusion in databases of Center participants, consultants, partners and stakeholders;
- to make appropriate logistical arrangements, whenever necessary;
- for future communication regarding updates related to Center programs/activities, as well as address queries and questions that may be received;
- to identify persons to contact in case of emergency; and
- to send evaluation instruments and other post-program/post-activity documents as needed.

The Center assures that these gathered information will only be used for non-commercial purposes. Adequate control, means and access to personal data are in place to ensure the safety, integrity and confidentiality of the said information.

Accuracy of Information

The Center strives to ensure that all personal data are current and accurate at the time of data collection. Any correction or update on an individual's personal information can be communicated to the Center through its designated Data Protection Officers (DPOs). Contact information of the Center's Personal Information Controller can be found on the last page of this Policy.

Storage and Retention

Personal data is stored and transmitted securely in a variety of paper and electronic formats, including databases that are shared between the Center's different units/offices. As may be provided by law, personal information may need to be retained indefinitely to satisfy legal obligations or for historical and statistical purposes.

Applicability

This Data Privacy Policy applies to personal information that the Center collects, processes and disposes of from staff, partners, consultants, stakeholders, etc. and in every SEAMEO INNOTECH activity, application, website, official social media site, and other points of contact.

Right of the Data Subject

Whenever sensitive personal information (i.e. marital status, education, health, social security number, tax identification number) is collected, efforts are in place to ensure that the participants, consultants, partners and other stakeholders (also called data subjects) are informed about:

- the project/ activity and the extent of the participation of the data subject, including the extent that shared information/ data will be used;
- the right to access data provided;
- the option to decline participation in the project/ activity for whatever reason;
- the right to erase or block any information earlier provided;
- the right to damages;
- the right to file a complaint;
- the right to rectify the information that they have shared/ provided; and
- the right to data portability.

If the sensitive personal information pertains to a minor or one who is not legally capable of entering into contractual transactions, the parent or guardian shall be responsible for giving the consent.

Responsibility of Center Staff and Partners

Center staff and partners who gather and handle data/personal information shall ensure that consent is secured from data subjects. Consent given by data subjects in whatever form are to be documented and supporting records should be readily retrievable. Those who process data shall ensure that protection is in place to avoid data breach. All equipment where personal data is stored shall be password protected while sensitive personal information on printed documents are to be kept in secure locations and disposed of using identified procedure. Security procedures shall also be applied in accessing personal information in the Center's online social media accounts/pages.

In cases of breach, the concerned staff or partner is responsible for reporting such to the DPOs as well as the Knowledge Management and Networking Office as all information breach may impact on the

image of the Center and require, if found necessary, the activation of the Crisis Communication Committee.

The Quality and Systems Management Office, through the concerned Internal Quality Audit Team Member, shall be informed as well for possible nonconformities and determine the root cause/s. The Systems Management Unit shall also be informed on issues concerning technology breach.

Data Privacy Impact and Risk Assessment

A Privacy Impact Assessment (PIA) shall, whenever deemed necessary, be undertaken in assessing potential impacts on privacy of any Center process, information systems, program, project, software, device and other initiatives which processes personal information.

The objective of a PIA is to identify and document information flows of personal information under assessment. In consultation with others in the organization, and as maybe applicable, others external to the organization, personal information flows are described and documented.

Handling and flow of personal information generated from programs, projects and other initiatives (including collection, storage, usage, retention, disclosure/sharing and disposal/destruction) should be tested for consistency with Data Privacy Principles.

Using the Center's established Risk Assessment and Management process and tools under its two ISO international standards, risks of unauthorized collection, use, disclosure or access to personal data, that could potentially result in harm or danger to a subject or the organization shall be assessed and managed. Included here is the risk that the confidentiality, integrity and availability of personal data will not be maintained, or the risk that processing will violate rights of data subjects or privacy principles of transparency, legitimacy and proportionality.

Inquiries and/or Concerns

For any other concern or question regarding personal rights or this Policy, please feel free to contact the Center's designated Personal Information Controller, Dr. Ramon C. Bacani, SEAMEO INNOTECH Director, with contact details as follows:

E-mail: privacy@seameo-innotech.org

Telephone: +63-2-924-7681 to 84

Facsimile: +63-2-921-0224